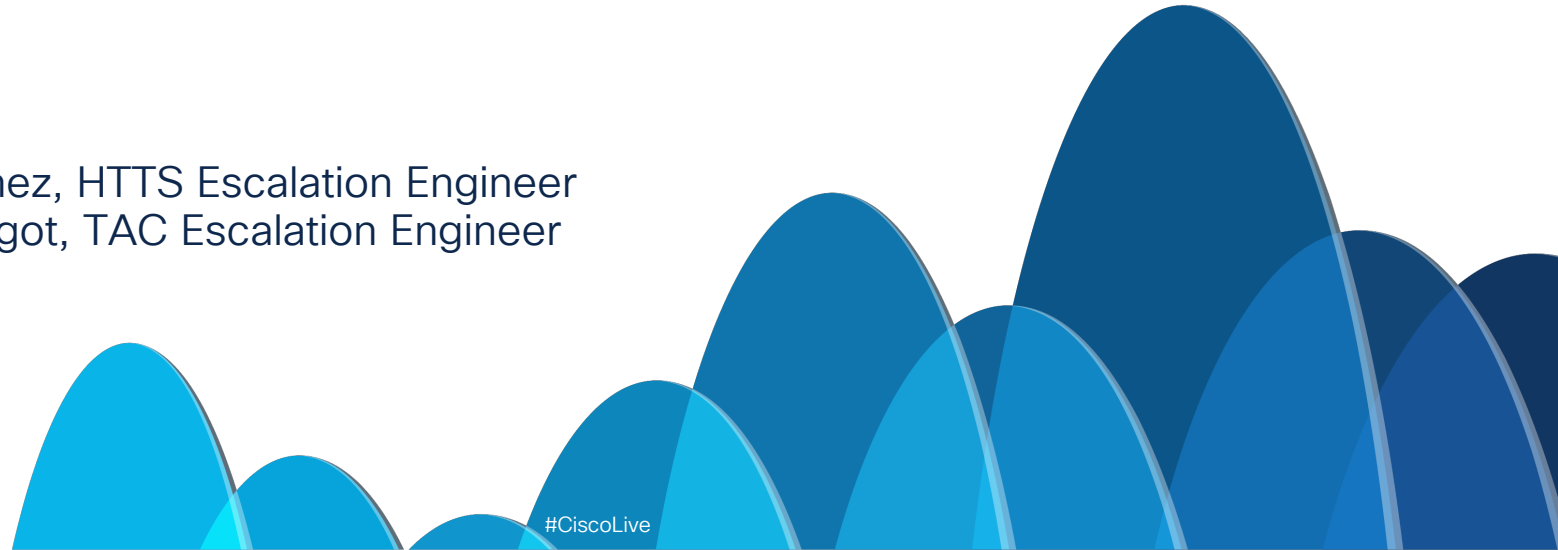
The bridge to possible

Configure, Verify, and Troubleshoot DIA in SD-WAN

Adrian Jimenez, HTTS Escalation Engineer
Connor Szurgot, TAC Escalation Engineer

TACENT-2014



cisco Live!

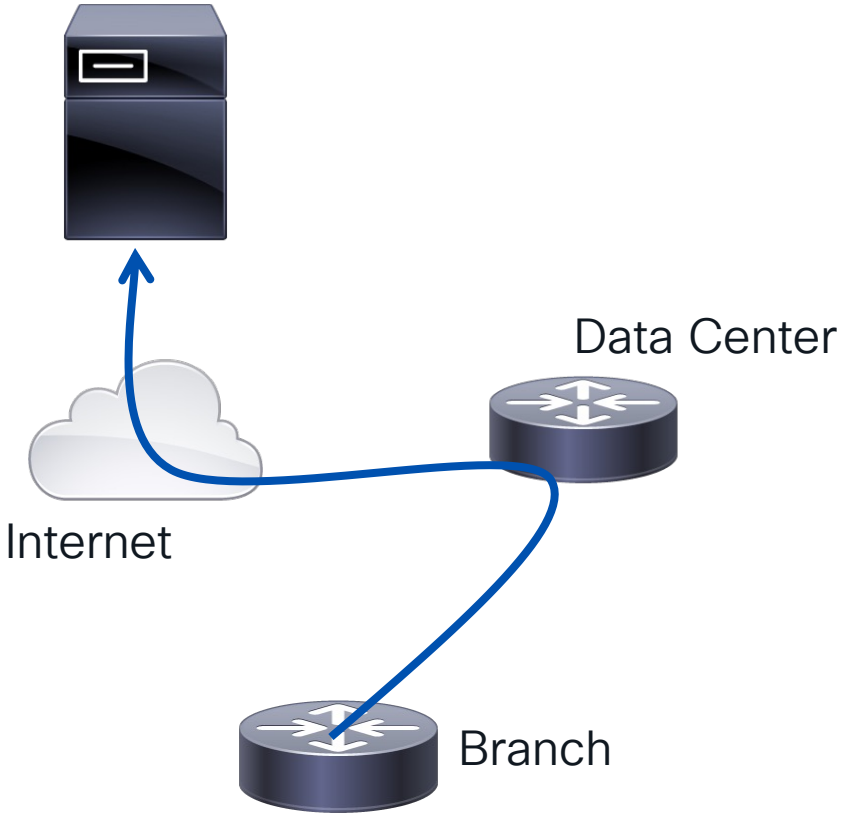
Agenda

- Introduction
- NAT DIA
- DIA via Route Leaking
- Additional Features for NAT DIA
- Q&A

What is Direct Internet Access (DIA)?

Problem

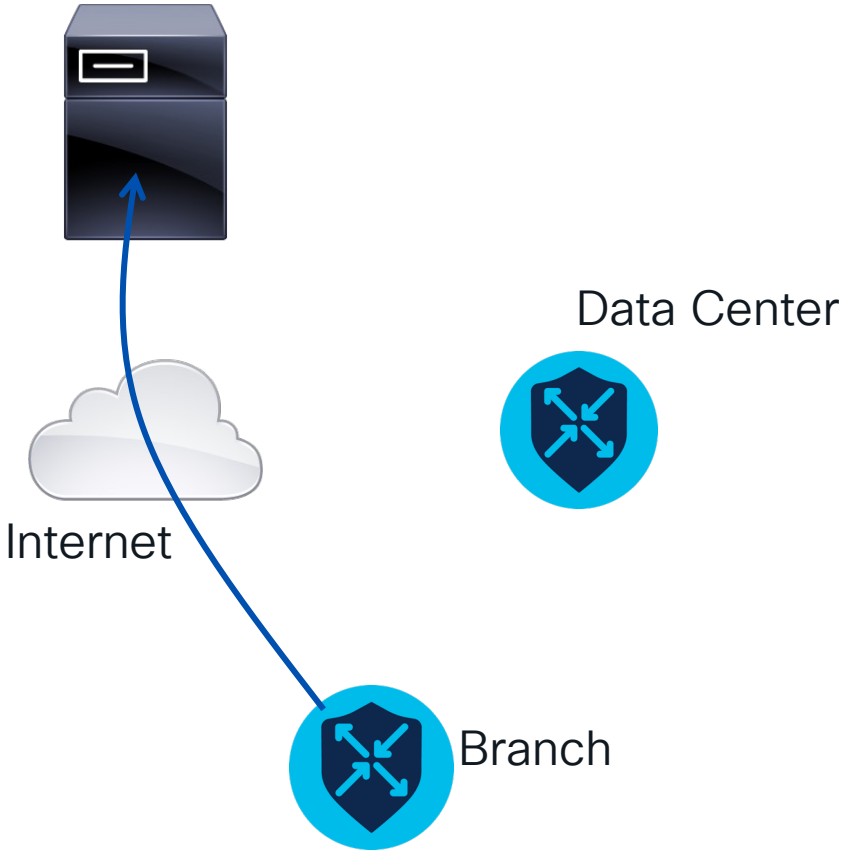
- Backhauling Traffic
- Slows Connections
- Costlier Links and Speeds Required at Data Center
- More Difficult to Scale



What is Direct Internet Access (DIA)?

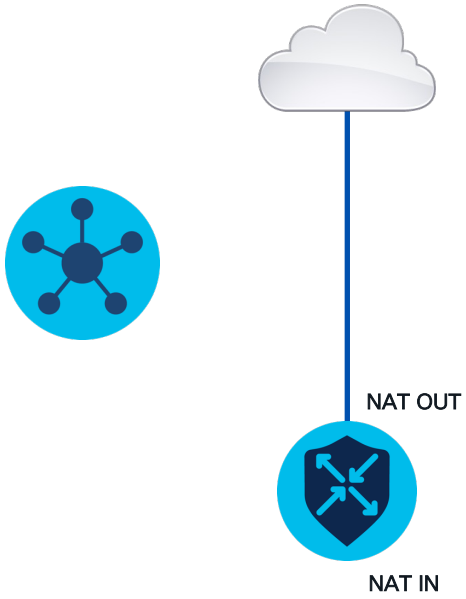
Solution

- Scales easily across any number of branches
- Faster Connections
- Avoids Backhauling



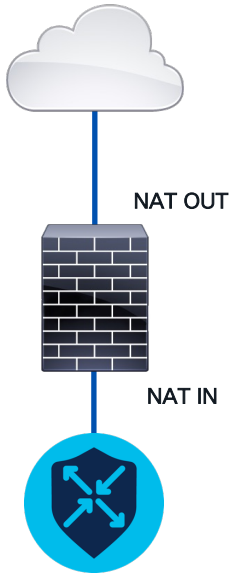
DIA Topologies

NAT DIA via Policy



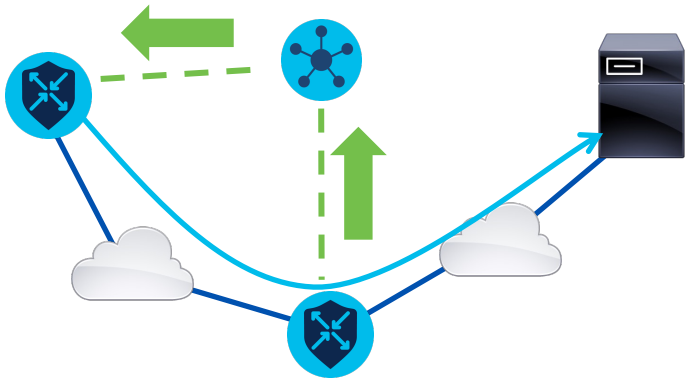
NAT DIA via Static Route

DIA via Route Leaking

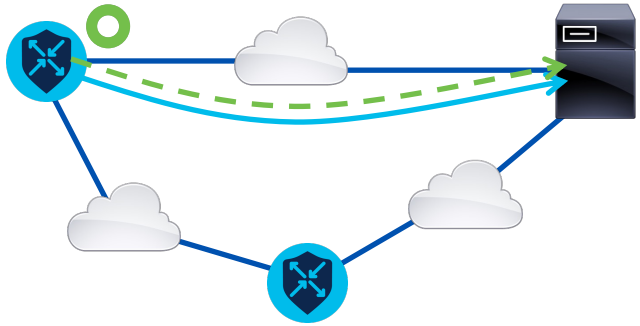


Additional NAT DIA Features

NAT Route Advertisement



Endpoint Tracker

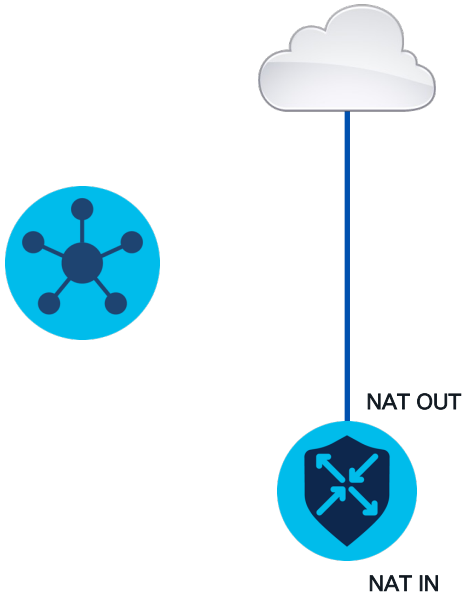


Device Assumptions

- Cisco IOS XE Catalyst SD-WAN Edge devices running 17.9
- SD-WAN Controllers running 20.9
- CLI configuration

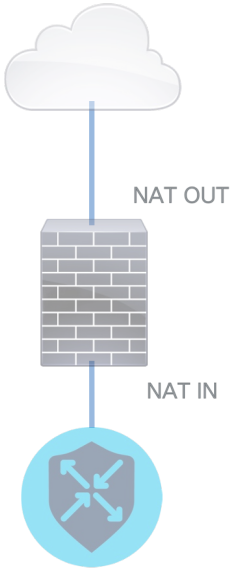
DIA Topologies

NAT DIA via Policy



NAT DIA via Static Route

DIA via Route Leaking

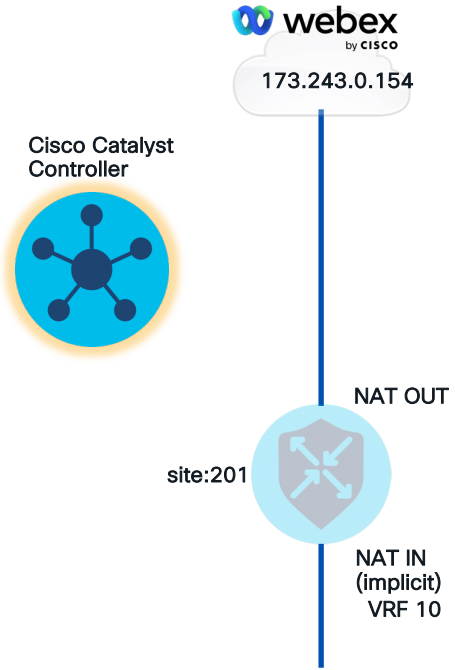


Configuration of NAT DIA via policy

Cisco Catalyst Controller configuration

1. Define lists/groups of interests:

```
vsmart#show running-config policy lists
policy
 lists
  vpn-list NAT_DIA_VPN
   vpn 10
  !
  data-prefix-list DIA_WBX
   ip-prefix 173.243.0.154/32
  !
  site-list DIA_Site_list
   site-id 201
   site-id 202
   site-id 203
```

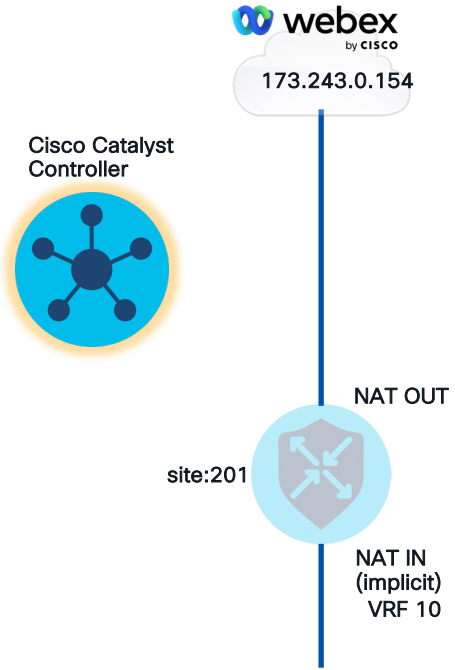


Configuration of NAT DIA via policy

Catalyst Controller configuration

2. Define DIA policy action (nat use-vpn 0):

```
vsmart# show running-config policy
policy
 data-policy NAT_DIA_POLICY
  vpn-list NAT_DIA_VPN
   sequence 10
    match
     destination-data-prefix-list DIA_WBX
    !
    action accept
     nat use-vpn 0
    !
   !
   default-action accept
```



3. Push policy to interested sites:

```
vsmart# show running-config apply-policy
apply-policy
 site-list DIA_Site_list
  data-policy NAT_DIA_POLICY from-service
```

Configuration of NAT DIA via policy

Cisco cEdge router configuration

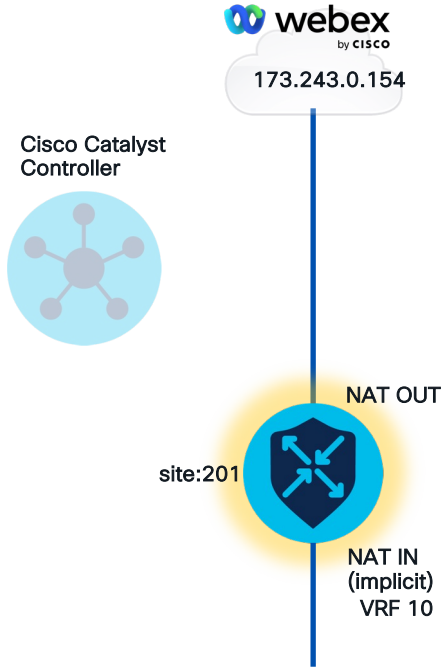
4. Traffic routed through outside interface gets evaluated against NAT statement

```
SDWAN-EDGE#(config)#interface GigabitEthernet1
SDWAN-EDGE#(config-if)#ip nat outside
```

5. NAT inside source references groups of interest defined in data policy not on ACL.

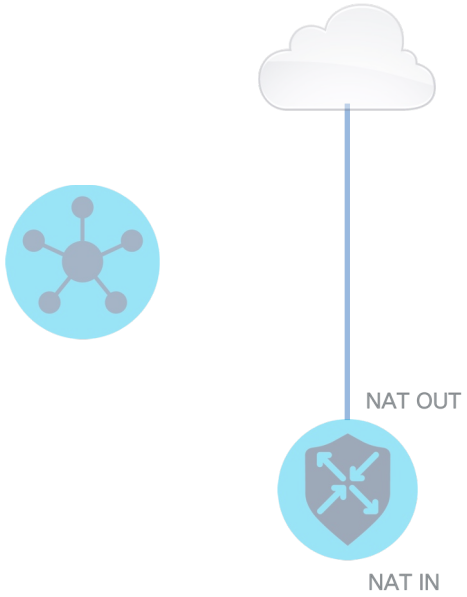
```
SDWAN-EDGE#(config)# ip nat inside source list nat-dia-list
interface GigabitEthernet1 overload
```

**The 'nat-dia-list' ACL is not explicitly configured; it is created internally as a "permit any any" configuring the NAT statement.*



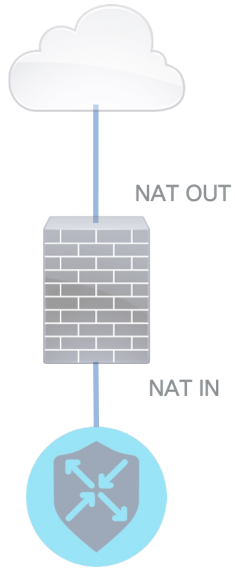
DIA Topologies

NAT DIA via Policy



NAT DIA via Static Route

DIA via Route Leaking



Configuration of NAT DIA via NAT route

1. Define outside interface

```
SDWAN-EDGE#(config)#interface GigabitEthernet1
SDWAN-EDGE#(config-if)#ip nat outside
```

2. Define NAT inside source

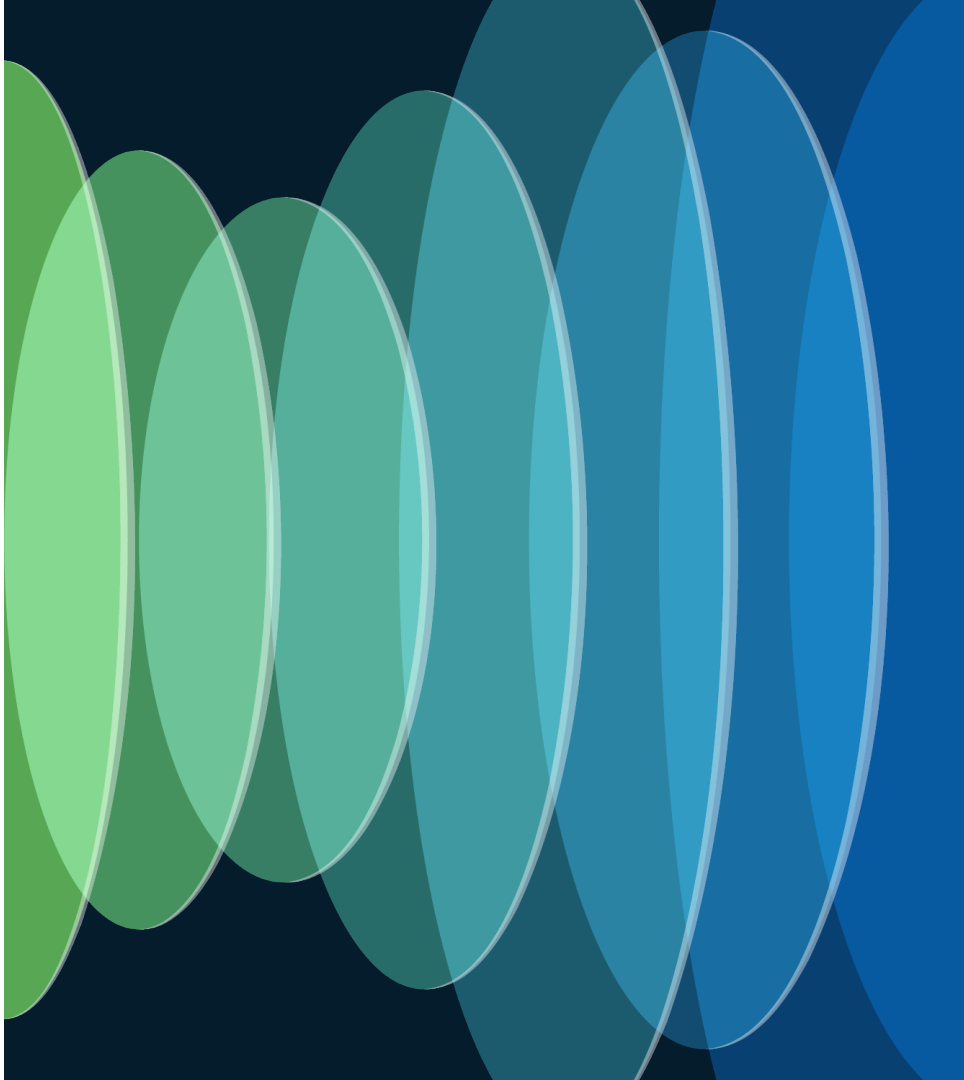
```
SDWAN-EDGE#(config)#ip nat inside source list nat-dia-vpn-hop-access-list
interface GigabitEthernet1 overload
```

3. Define NAT route

```
SDWAN-EDGE#(config)#ip nat route vrf 10 173.243.0.154 255.255.255.255 global
OR
SDWAN-EDGE#(config)#ip nat route vrf 10 0.0.0.0 0.0.0.0 global
```

**If running a routing protocol on the service-side (LAN side), ensure that this route is redistributed into it. Use "*redistribute nat-route dia" command to do so.

NAT DIA Verification



Verification of NAT DIA

Checking NAT DIA/Route Commands on cEdge

- **“show sdwan policy from-vsmart”**
- “show ip nat statistics”
- “show ip nat translations”

```
SDWAN-EDGE#show sdwan policy from-vsmart
from-vsmart data-policy NAT_DIA_POLICY
 direction from-service
 vpn-list NAT_DIA_VPN
  sequence 20
   match
    destination-data-prefix-list DIA_WBX
   action accept
    nat use-vpn 0
    no nat fallback
  default-action accept

from-vsmart lists vpn-list NAT_DIA_VPN
 vpn 10

from-vsmart lists data-prefix-list DIA_WBX
 ip-prefix 173.243.0.154/32
```

Verification of NAT DIA

Checking NAT DIA/Route Commands on cEdge

- “show sdwan policy from-vsmart”
- **“show ip nat statistics”**
- “show ip nat translations”

```
SDWAN-EDGE#show ip nat statistics
Total active translations: 1 (0 static, 1 dynamic;
1 extended)
Outside interfaces:
  GigabitEthernet1
Inside interfaces:
Hits: 1621  Misses: 1461
Expired translations: 1442
Dynamic mappings:
-- Inside Source
[Id: 9] access-list nat_route interface
GigabitEthernet1 refcount 1
nat-limit statistics:
 max entry: max allowed 0, used 0, missed 0
In-to-out drops: 0  Out-to-in drops: 0
Pool stats drop: 0  Mapping stats drop: 0
Port block alloc fail: 0
IP alias add fail: 0
Limit entry add fail: 0
```

Verification of NAT DIA

Checking NAT DIA on cEdge

- “show sdwan policy from-vsmart”
- “show ip nat statistics”
- “**show ip nat translations**”

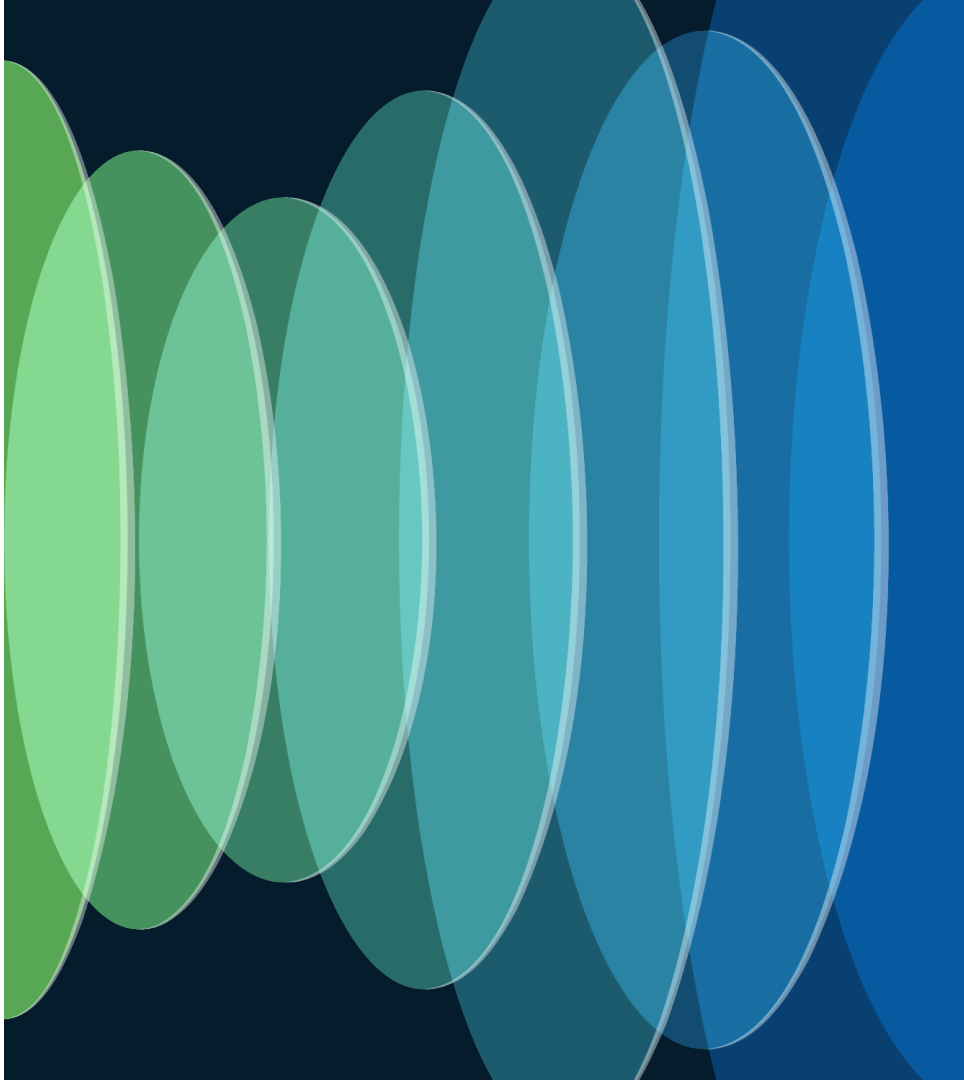
```
SDWAN-EDGE#show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
icmp 192.168.30.18:59      172.16.123.1:59       173.243.0.154:59      173.243.0.154:59
Total number of translations: 1
```

Verification of NAT DIA

Checking NAT Route

```
cedge1_17_9_1a#show ip route vrf 10 <nat-route>

Routing Table: 10
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

n*Nd  0.0.0.0/0 [6/0], 00:02:59, Null0
<output omitted>
n Nd     173.243.0.154 [6/0], 00:04:04, Null0
```

Troubleshooting NAT DIA



Troubleshoot with the IOS-XE Datapath Packet (FIA) Trace

https://www.cisco.com/c/en/us/support/docs/content-networking/adaptive-session-redundancy-asr/117858-technote-asr-00.html

FIA Trace Overview

1. Configure a Filter

```
debug platform condition ipv4 173.243.0.154/32 both
```

2. Configure the Trace

```
debug platform condition packet-trace packet 1024 fia-trace
```

3. Start the Trace

```
debug platform condition [start|stop]
```

4. Dump the Packets

```
show platform packet-trace summary
Show platform packet-trace packet [#|all]
```

Troubleshooting NAT DIA

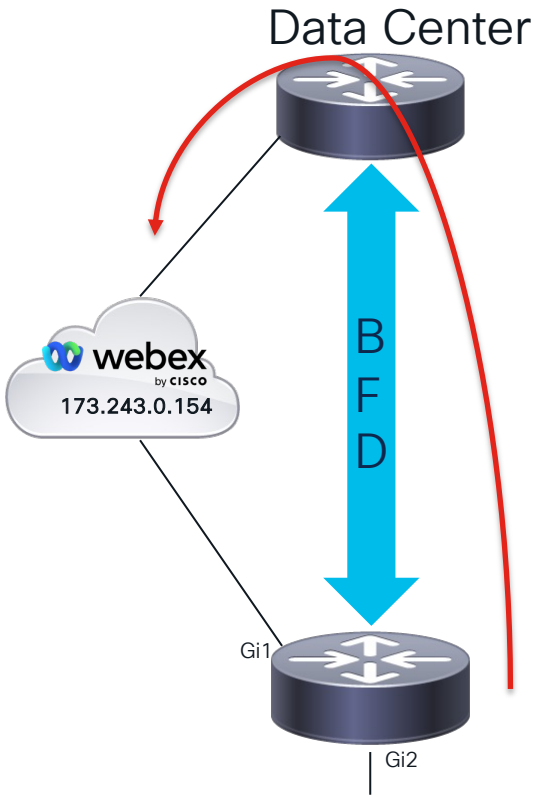
Using FIA trace to check Policy/Routing Matching

Problem

Connections to cloud applications and internet is slow.

Troubleshooting

- Not seeing NAT translations entries for the DIA interested traffic.
- Internet traffic is hitting DC/Hub before getting to the internet



Troubleshoot NAT DIA

Traffic going to overlay instead of DIA

```
SDWAN-EDGE# show platform packet-trace packet 0
  Input      : GigabitEthernet2 ──→ VRF 10
  Output     : GigabitEthernet1 ──→ VRF 0
  State      : FWD
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet2
    Output      : <unknown>
    Source      : 172.16.123.1
    Destination : 173.243.0.154
    Protocol    : 1 (ICMP)
Feature: SDWAN Data Policy IN
    VPN ID      : 10
    VRF         : 3
    Policy Name : NAT_DIA_POLICY-NAT_DIA_VPN (CG:4)
    Seq         : Default
Feature: SDWAN Forwarding
    SDWAN adj OCE:
    Output      : GigabitEthernet1
    Hash Value  : 0xca
    Encap       : ipsec
    SLA         : 0
    SDWAN VPN   : 10
    SDWAN Proto : IPV4
    Out Label   : 45566
    Local Color : biz-internet
    Remote Color : biz-internet
```

```
SDWAN-EDGE#show platform packet-trace packet 1
Packet: 1           CBUG ID: 19696671
Summary
  Input      : Tunnel1
  Output     : GigabitEthernet2
  State      : FWD
  Timestamp
Path Trace
  Feature: IPV4(Output)
    Input       : Tunnel1
    Output      : GigabitEthernet2
    Source      : 173.243.0.154
    Destination : 172.16.123.1
    Protocol    : 1 (ICMP)
```

How to FIA trace

Troubleshoot NAT DIA

Traffic going to overlay instead of DIA

```
SDWAN-EDGE# show platform packet-trace packet 0
  Input      : GigabitEthernet2  ──► VRF 10
  Output     : GigabitEthernet1  ──► VRF 0
  State      : FWD
Path Trace
  Feature: IPV4(Input)
    Input        : GigabitEthernet2
    Output       : <unknown>
    Source       : 172.16.123.1
    Destination  : 173.243.0.154
    Protocol     : 1 (ICMP)
Feature: SDWAN Data Policy IN
    VPN ID       : 10
    VRF          : 3
    Policy Name  : NAT_DIA_POLICY-NAT_DIA_VPN (CG:4)
    Seq          : Default
Feature: SDWAN Forwarding
    SDWAN adj OCE:
    Output       : GigabitEthernet1
    Hash Value   : 0xca
    Encap        : ipsec
    SLA          : 0
    SDWAN VPN    : 10
    SDWAN Proto  : IPV4
    Out Label    : 45566
    Local Color  : biz-internet
    Remote Color : biz-internet
```

```
SDWAN-EDGE#show sdwan policy from-vsmart
from-vsmart data-policy NAT_DIA_POLICY
 direction from-service
 vpn-list NAT_DIA_VPN
  sequence 20
   match
    destination-data-prefix-list DIA_ALLOW_PRFX
   action accept
    nat use-vpn 0
    no nat fallback
  default-action accept

from-vsmart lists vpn-list NAT_DIA_VPN
 vpn 10

from-vsmart lists data-prefix-list DIA_ALLOW_PRFX
 ip-prefix 192.168.0.0/16
```

Troubleshoot NAT DIA

Fixing policy for proper sequence matching

```
SDWAN-EDGE#show platform packet-trace packet 2
<… output omitted …>
  Input     : GigabitEthernet2
  Output    : GigabitEthernet1
  State     : FWD
<… output omitted …>
 Feature: SDWAN Data Policy IN
    VPN ID       : 10
    VRF          : 3
    Policy Name  : NAT_DIA_POLICY-NAT_DIA_VPN (CG:4)
    Seq          : 20
    DNS Flags    : (0x0) NONE
    Policy Flags : 0x10
    Nat Map ID   : 1
    SNG ID       : 0
    Action       : REDIRECT_NAT
 Feature: NAT
    VRFID          : 3
    table-id       : 3
    Protocol       : ICMP
    Direction      : IN to OUT
    From           : Service side
    Action         : Translate Source
    Steps          : SESS-CREATE
    Match id       : 9
    Old Address    : 172.16.123.1
    New Address    : 192.168.30.18
```

```
SDWAN-EDGE#show platform packet-trace packet 3
<… output omitted …>
 Feature: SDWAN Implicit ACL
    Action : ALLOW
    Reason : SDWAN_NAT_DIA
 Feature: NAT
    VRFID          : 0
    table-id       : 0
    Protocol       : ICMP
    Direction      : OUT to IN
    From           : DIA INTERFACE
    Action         : Translate Destination
    Steps          :
    Match id       : 9
    Old Address    : 192.168.30.18
    New Address    : 172.16.123.1
```

How to FIA trace

Troubleshoot NAT DIA

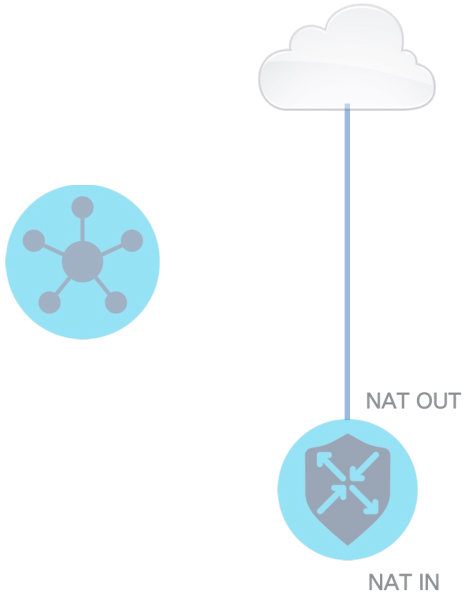
Fixing policy for proper sequence matching

```
SDWAN-EDGE#show platform packet-trace packet 2
<… output omitted …>
  Input      : GigabitEthernet2
  Output     : GigabitEthernet1
  State      : FWD
<… output omitted …>
 Feature: SDWAN Data Policy IN
    VPN ID       : 10
    VRF          : 3
    Policy Name  : NAT_DIA_POLICY-NAT_DIA_VPN (CG:4)
    Seq          : 20
    DNS Flags    : (0x0) NONE
    Policy Flags : 0x10
    Nat Map ID   : 1
    SNG ID       : 0
    Action       : REDIRECT_NAT
 Feature: NAT
    VRFID          : 3
    table-id       : 3
    Protocol       : ICMP
    Direction      : IN to OUT
    From           : Service side
    Action         : Translate Source
    Steps          : SESS-CREATE
    Match id       : 9
    Old Address    : 172.16.123.1
    New Address    : 192.168.30.18
```

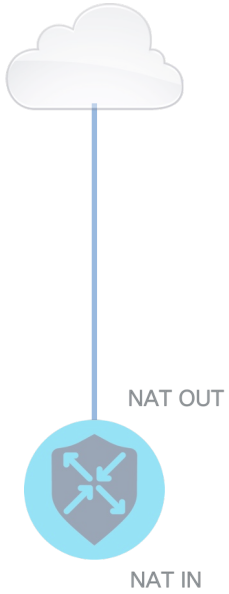
```
SDWAN-EDGE#show sdwan policy from-vsmart
from-vsmart data-policy NAT_DIA_POLICY
 direction from-service
 vpn-list NAT_DIA_VPN
  sequence 20
   match
    destination-data-prefix-list DIA_WBX
   action accept
    nat use-vpn 0
    no nat fallback
  default-action accept

from-vsmart lists vpn-list NAT_DIA_VPN
 vpn 10

from-vsmart lists data-prefix-list DIA_WBX
 ip-prefix 173.243.0.154/32
```

DIA Topologies

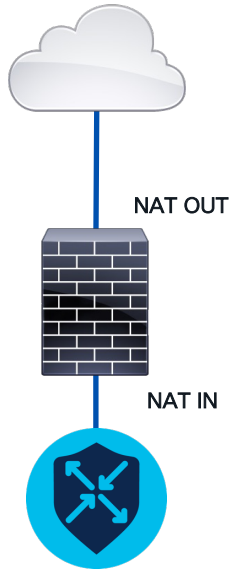
NAT DIA via Policy



NAT DIA via Static Route



DIA via Route Leaking



Configuration of DIA via Route Leaking

1. Leak the routes from the transport (global) VRF to the service (10) VRF

```
vrf definition 10
 address-family ipv4
  route-replicate from vrf global unicast <protocol>
  exit-address-family
 !
```

2. Leak the routes from the service (10) VRF to the transport (global) VRF

```
global-address-family ipv4
 route-replicate from vrf 10 unicast <protocol>
 exit-global-af
!
```

Verification of DIA via Route Leaking

Before

```
SDWAN-EDGE#show ip route
<… output omitted …>
Gateway of last resort is 172.16.0.1 to network 0.0.0.0 <<< Default route to leak

S*    0.0.0.0/0 [1/0] via 172.16.0.1
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.0.0/24 is directly connected, GigabitEthernet1
L        172.16.0.2/32 is directly connected, GigabitEthernet1


SDWAN-EDGE#show ip route vrf 10
<… output omitted …>
Gateway of last resort is not set <<< No default route for service-side

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.0.0.0/28 is directly connected, GigabitEthernet2 <<< Service-side route to leak
L        10.0.0.1/32 is directly connected, GigabitEthernet2
```

Verification of DIA via Route Leaking

After

```
SDWAN-EDGE#sh ip route
<… output omitted …>
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is 172.16.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.0.1
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C   +    10.0.0.0/28 is directly connected, GigabitEthernet2 <<< Access back to service
L   &    10.0.0.1/32 is directly connected, GigabitEthernet2
 172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.0.0/24 is directly connected, GigabitEthernet1
L        172.16.0.2/32 is directly connected, GigabitEthernet1

SDWAN-EDGE#sh ip route vrf 10
<… output omitted …>
Gateway of last resort is 172.16.0.1 to network 0.0.0.0 <<< Default route leaked

S*  + 0.0.0.0/0 [1/0] via 172.16.0.1
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.0.0.0/28 is directly connected, GigabitEthernet2
L        10.0.0.1/32 is directly connected, GigabitEthernet2connected, GigabitEthernet1
```

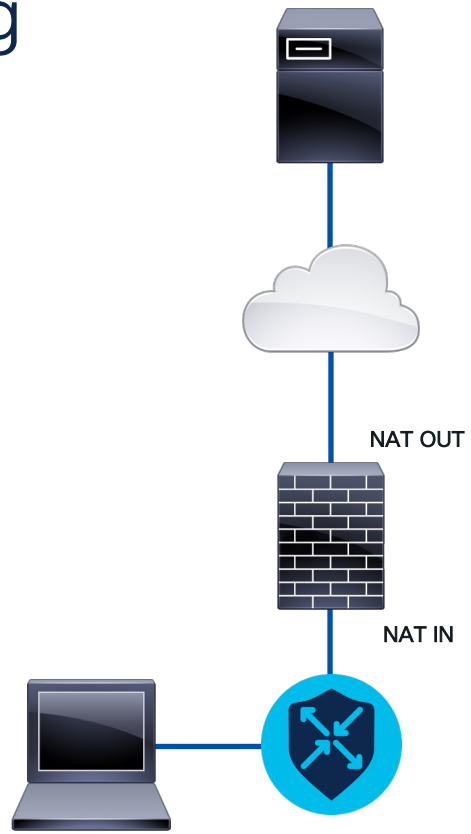
Troubleshoot DIA via Route Leaking

Problem

The user is unable to ping the public internet server.

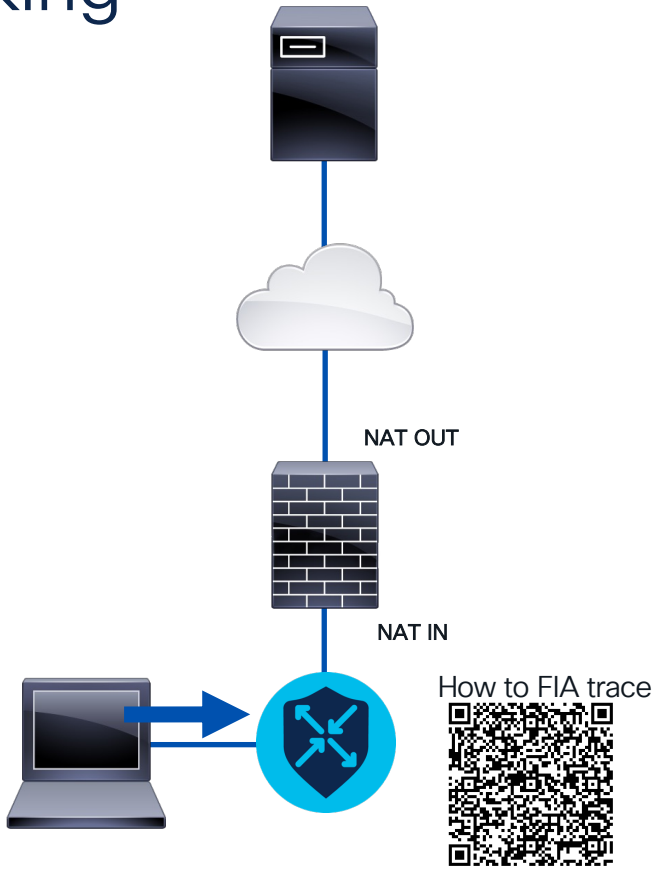
Troubleshooting

- User can ping default gateway.
- Firewall sees NAT entries being created.
- WAN-side packet capture on the SD-WAN router sees bi-directional traffic.



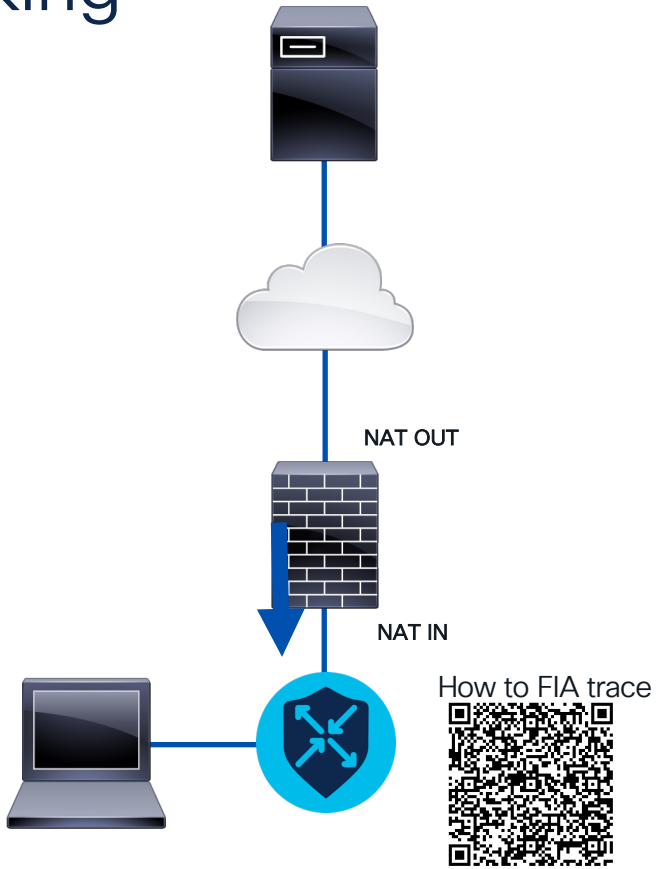
Troubleshoot DIA via Route Leaking

```
SDWAN-EDGE#sh platform packet-trace packet 0
Packet: 0            CBUG ID: 0
Summary
  Input     : GigabitEthernet2  ← VRF 10
  Output    : GigabitEthernet1  ← VRF 0
  State     : FWD
<… output omitted …>
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet2
    Output      : <unknown>
    Source      : 10.0.0.2        ← Client
    Destination : 192.168.1.1     ← Internet Server
    Protocol    : 1 (ICMP)
```



Troubleshoot DIA via Route Leaking

```
SDWAN-EDGE#show platform packet-trace packet 1
Packet: 1            CBUG ID: 1
Summary
  Input      : GigabitEthernet1 ← Same if
  Output     : GigabitEthernet1
  State      : FWD
<… output omitted …>
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet1
    Output      : <unknown>
    Source      : 192.168.1.1
    Destination : 10.0.0.2
    Protocol    : 1 (ICMP)
<… output omitted …>
 Feature: IPV4_INPUT_LOOKUP_PROCESS
    Entry       : Input - 0x81464e00
    Input       : GigabitEthernet1
    Output      : GigabitEthernet1
    Lapsed time : 495 ns
```



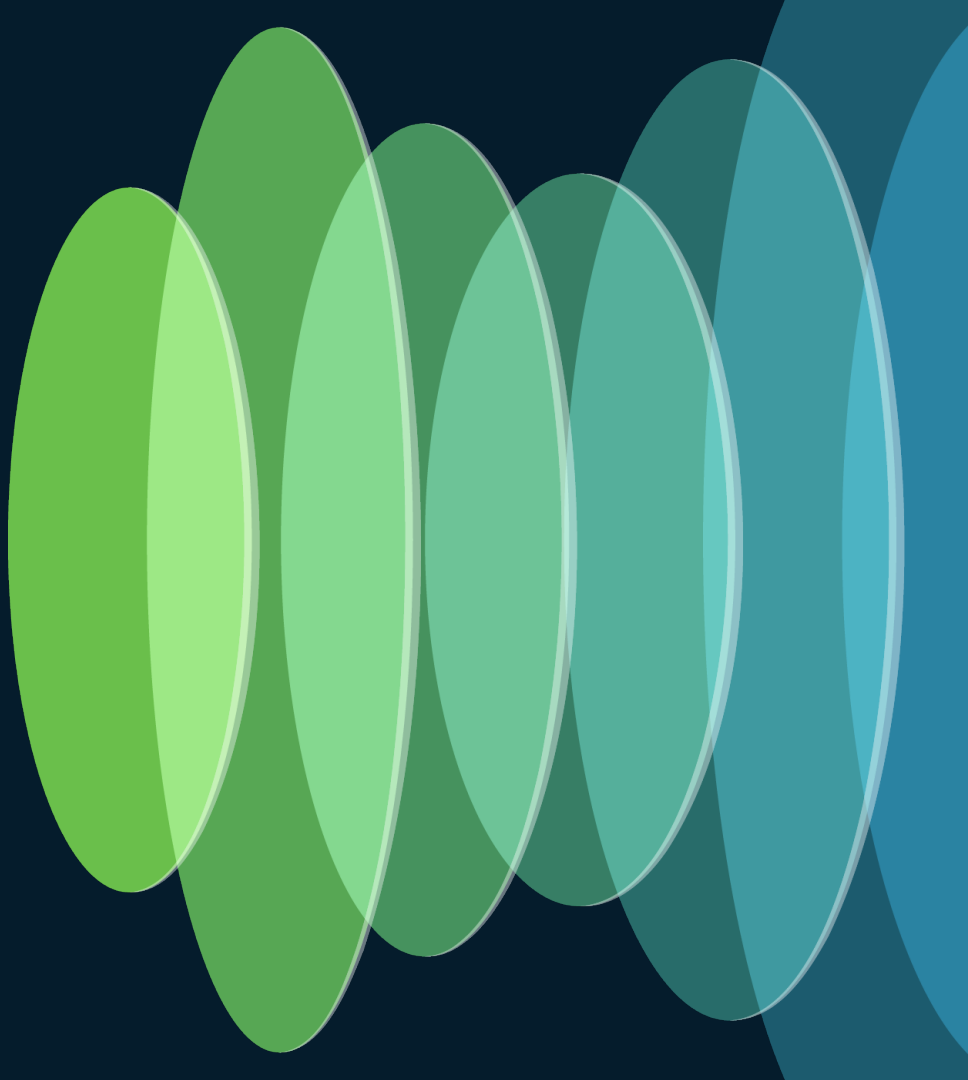
Troubleshoot DIA via Route Leaking

```
SDWAN-EDGE#sh ip route
<… output omitted …>
Gateway of last resort is 172.16.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.0.1
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.0.0/24 is directly connected, GigabitEthernet1
L        172.16.0.2/32 is directly connected, GigabitEthernet1

SDWAN-EDGE#sh run | s vrf definition 10|global-address-family
vrf definition 10
 !
 address-family ipv4
  route-replicate from vrf global unicast static
 exit-address-family
<<< No leaking from service to global
```

Solution:

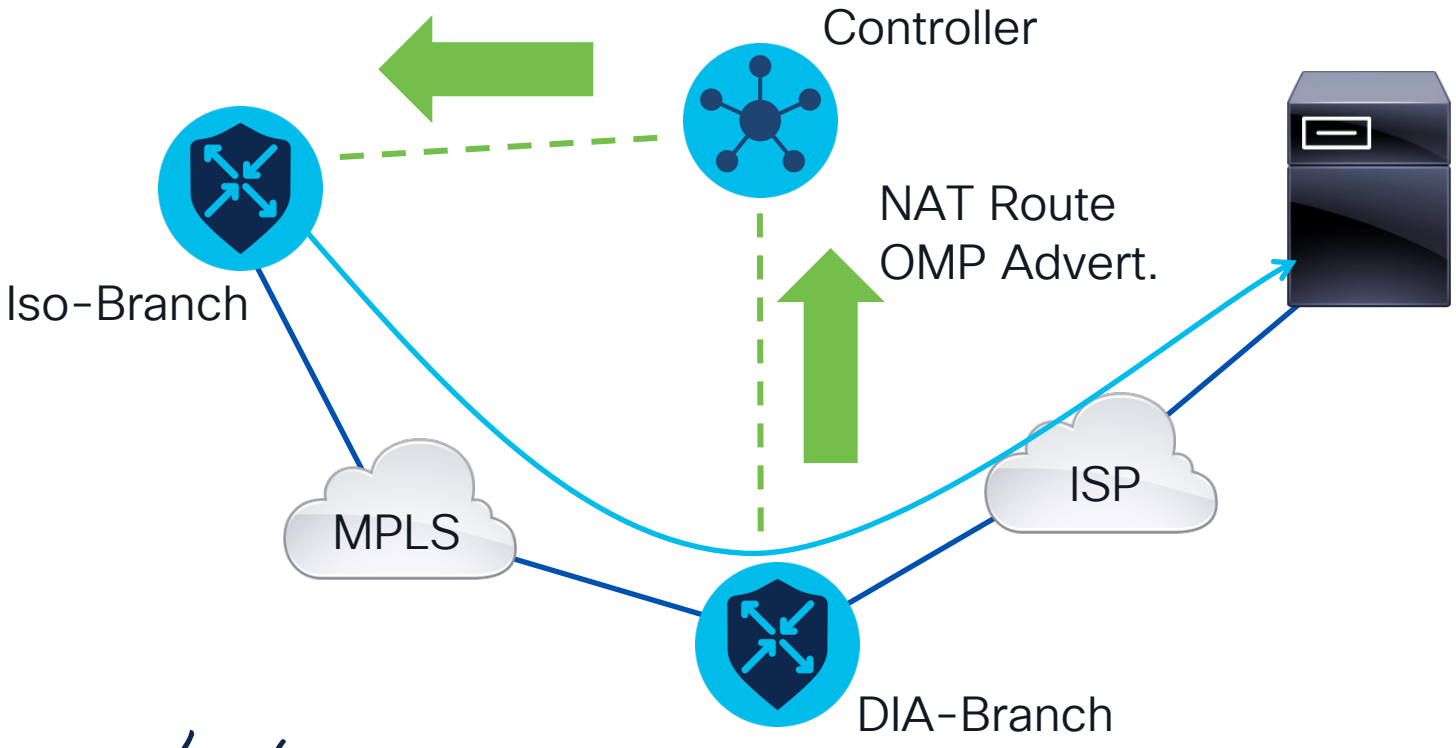
```
global-address-family ipv4
 route-replicate from vrf 10 unicast <protocol>
 exit-global-af
!
```

Additional Features for NAT DIA



Additional NAT DIA Features

OMP Advertisement of NAT Route



NAT Route Advertisement via OMP

- Allows you to advertise a routes DIA route across the overlay
- Allows routers to act as DIA hubs or backup paths for the overlay network.

```
! NAT DIA via Static Route Already Configured
!
! Advertise Route
sdwan
 omp
  address-family ipv4 vrf 10
   advertise network 0.0.0.0/0
  !
 !
!
```

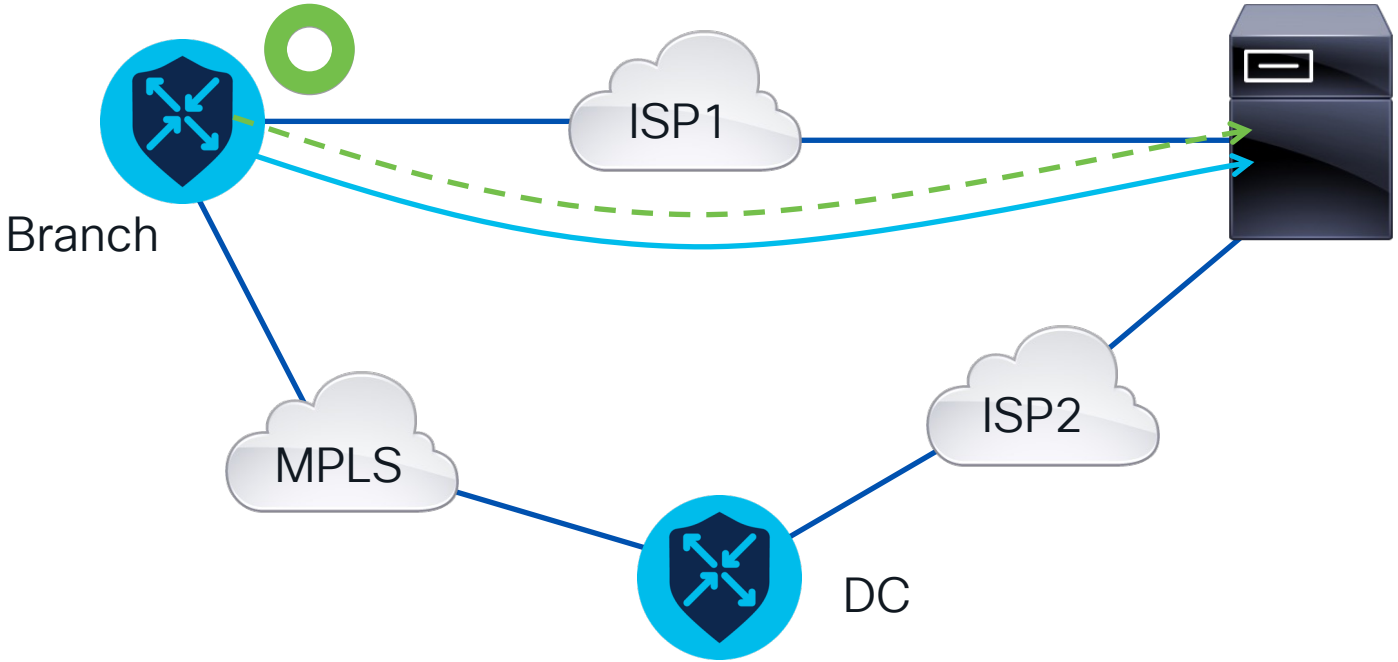
NAT Route Advertisement via OMP

Verification

```
ISO-BRANCH#sh sdwan omp routes vpn 10 0.0.0.0/0 detail

---------------------------------------------------------------------------
omp route entries for tenant-id 0 vpn 10 route
---------------------------------------------------------------------------
            RECEIVED FROM:
peer            10.0.0.3
path-id         3
label           1003
status          C,I,R <<< 'I' for installed
<… output omitted …>
    Attributes:
     originator       10.0.0.1
     type             installed
     tloc             10.0.0.1, biz-internet, ipsec
     <… output omitted …>
     site-id          201
     <… output omitted …>
     origin-proto     nat-dia
     origin-metric    0
     <… output omitted …>
```

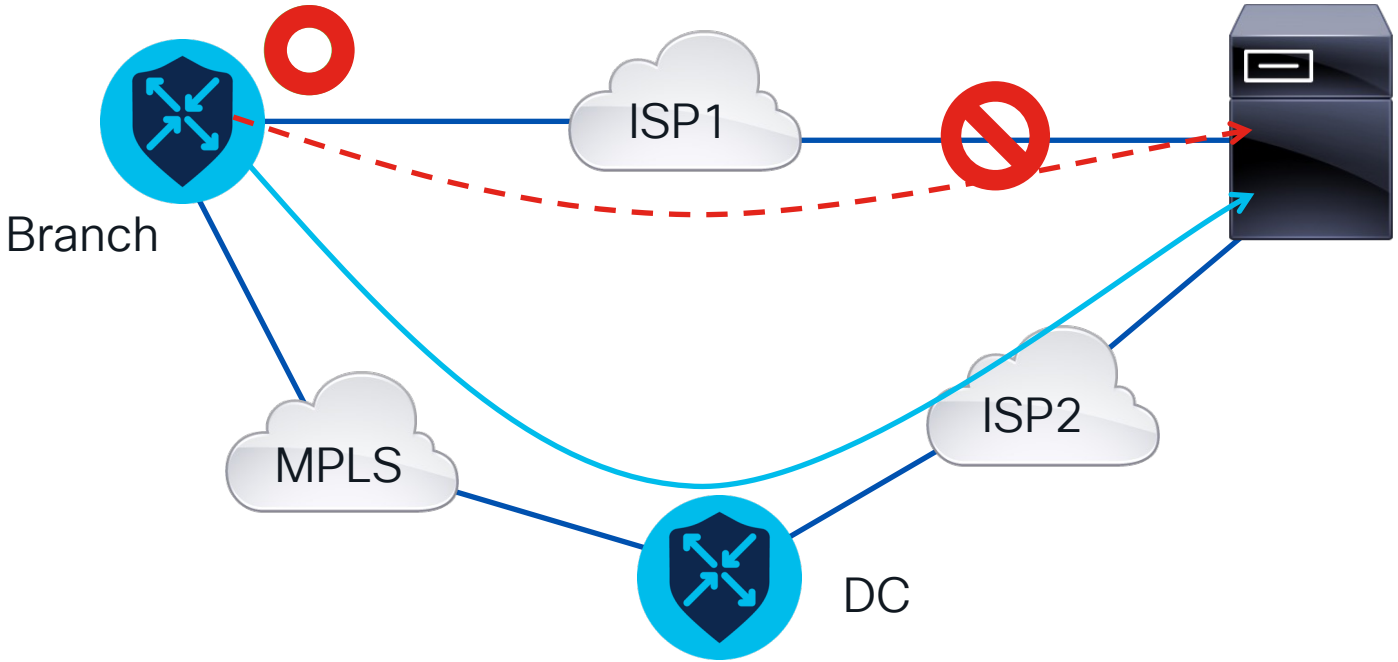
Additional NAT DIA Features

Endpoint Tracker



Additional NAT DIA Features

Endpoint Tracker



Endpoint Tracker

- Tracks the reachability of an endpoint on the internet as a test of the ability of this interface to provide DIA.
- If the endpoint is unreachable, don’t sent DIA traffic via this interface.

```
! Define Tracker
endpoint-tracker <name>
 endpoint-dns-name www.cisco.com
 interval 20
 threshold 200
 multiplier 2
 tracker-type interface

! Apply Tracker
interface GigabitEthernetX
 ip nat outside
 endpoint-tracker <name>
```

Endpoint Tracker

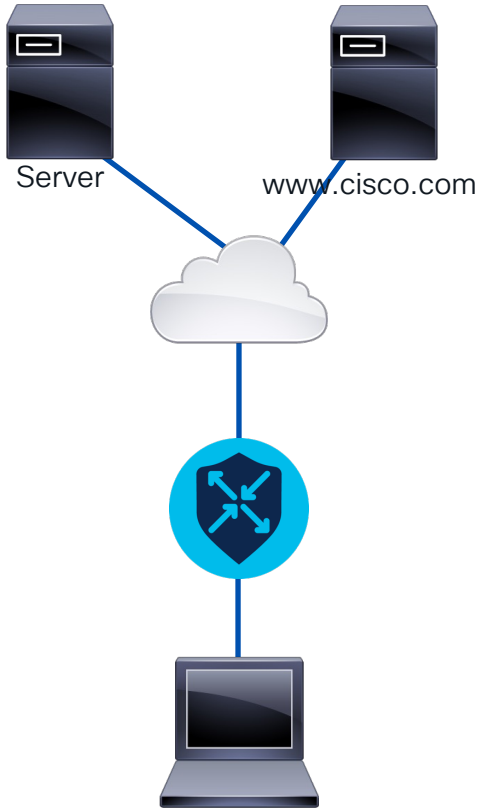
Troubleshooting - Scenario #1

Problem

Users are reporting that they are unable to access the internet.

Troubleshooting

- I can ping internet IP address from VPN0 on the router.
- My internet reliant BFD sessions are still up.



Endpoint Tracker

Troubleshooting - Scenario #1

```
SDWAN-EDGE#show ip route vrf 10
<… output omitted …>
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.0.0.0/28 is directly connected, GigabitEthernet2
L        10.0.0.1/32 is directly connected, GigabitEthernet2

SDWAN-EDGE#show endpoint-tracker
Interface              Record Name            Status          RTT in msecs    Probe ID        Next Hop
GigabitEthernet1       INET                   Down            Timeout         7               172.16.0.1

SDWAN-EDGE#show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending
All Stats are in milliseconds. Stats with u are in microseconds

ID           Type        Destination       Stats       Return          Last
                                                       Code            Run
------------------------------------------------------------------------------
*7           http        0.0.0.0           RTT=0       DNS query error 20 seconds ago
```

Endpoint Tracker

Troubleshooting - Scenario #1

```
SDWAN-EDGE#show endpoint-tracker records
Record Name      Endpoint           EndPoint Type   Threshold(ms)    Multiplier   Interval(s) Tracker-Type
INET             www.cisco.com      DNS_NAME        200              2            20          interface

SD-WAN-Hub#sh ip dns view
DNS View default parameters:
DNS Resolver settings:
  Domain lookup is enabled
  Default domain name:
  Domain search list:
  Domain name-servers:
    192.168.1.1


SDWAN-EDGE#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.128.1.1, timeout is 2 seconds:
..... <<< Unreachable
```

Endpoint Tracker

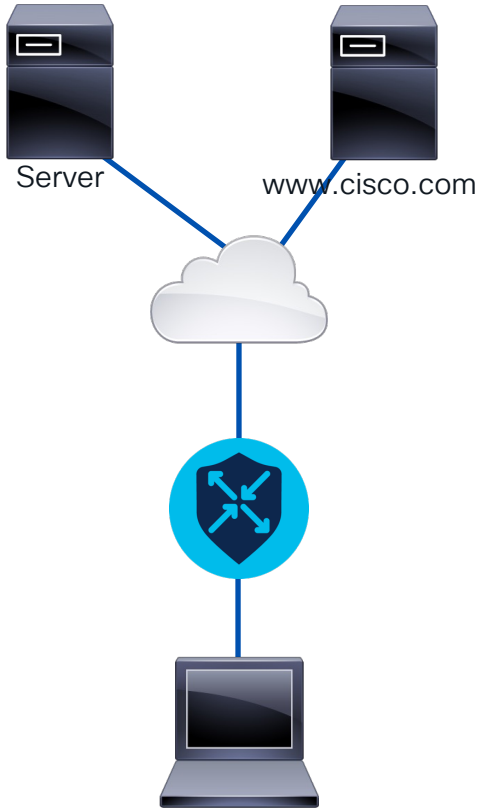
Troubleshooting - Scenario #2

Problem

Users are reporting that they are unable to access the internet.

Troubleshooting

- I can ping internet IP address from VPN0 on the router.
- My internet reliant BFD sessions are still up.



Endpoint Tracker

Troubleshooting - Scenario #2

```
SDWAN-EDGE#show ip route vrf 10
<… output omitted …>
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.0.0.0/28 is directly connected, GigabitEthernet2
L        10.0.0.1/32 is directly connected, GigabitEthernet2
```

```
SDWAN-EDGE#sh endpoint-tracker
Interface              Record Name            Status          RTT in msecs    Probe ID        Next Hop
GigabitEthernet1       INET                   Down            Timeout         7               172.16.0.1
```

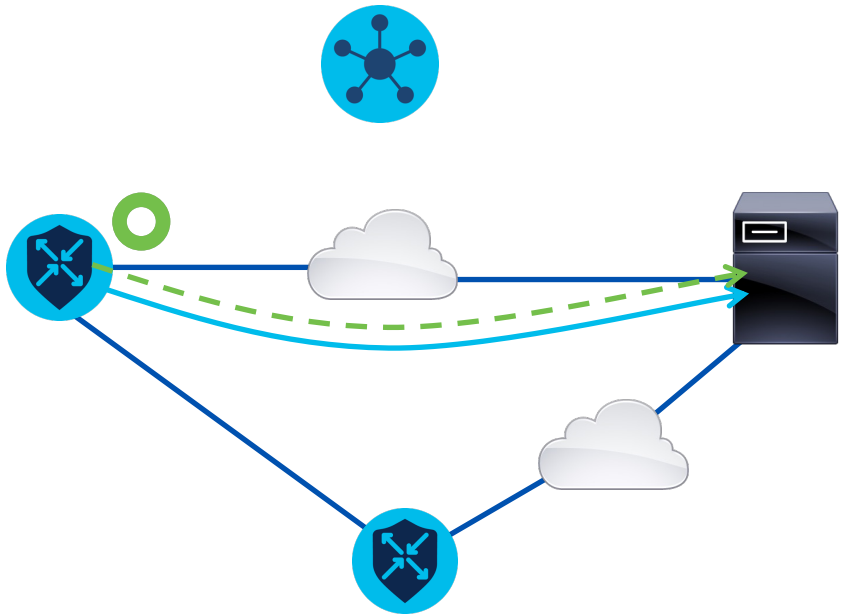
Endpoint Tracker

Troubleshooting - Scenario #2

```
SDWAN-EDGE#sh ip sla summ
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending
All Stats are in milliseconds. Stats with u are in microseconds

ID           Type        Destination       Stats       Return          Last
                                                       Code            Run
---------------------------------------------------------------------------
*7           http        192.168.0.1       RTT=917     Over threshold 2 seconds ago


SDWAN-EDGE#sh endpoint-tracker records
Record Name    Endpoint      EndPoint Type  Threshold(ms)  Multiplier  Interval(s)  Tracker-Type
INET           192.168.0.1   IP             300            3           60           interface
```

Continue Learning

- Configuration Guide: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/nat/nat-book-xe-sdwan/configure-nat.html#service-side-nat
- Cisco Validated Design: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sdwan-dia-deploy-2020aug.pdf
- GUI Reference: https://www.cisco.com/c/en/us/support/docs/routers/xe-sd-wan-routers/220613-implement-direct-internet-access-dia-f.html



Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact us at:

Adrian Jimenez – adrjimen@cisco.com

Connor Szurgot – cszurgot@cisco.com

Complete Your Session Evaluations

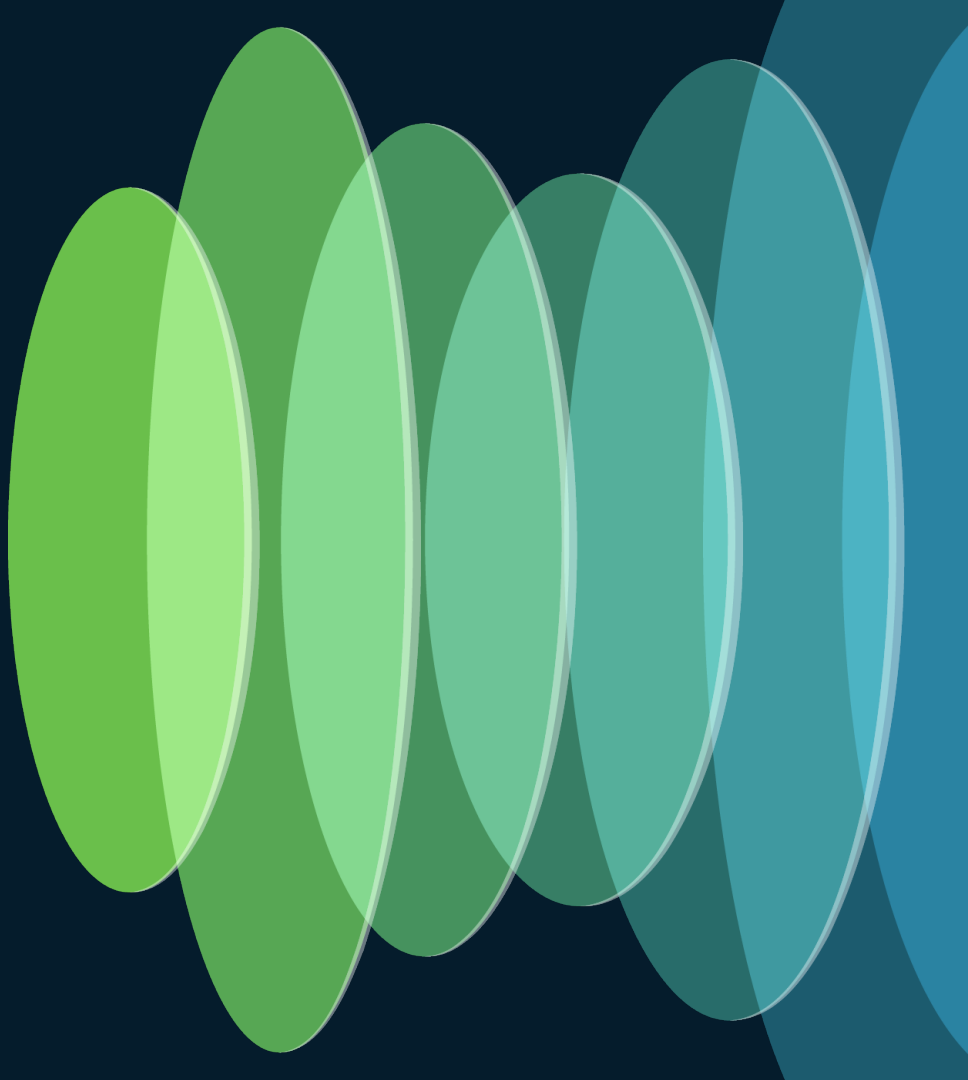
Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

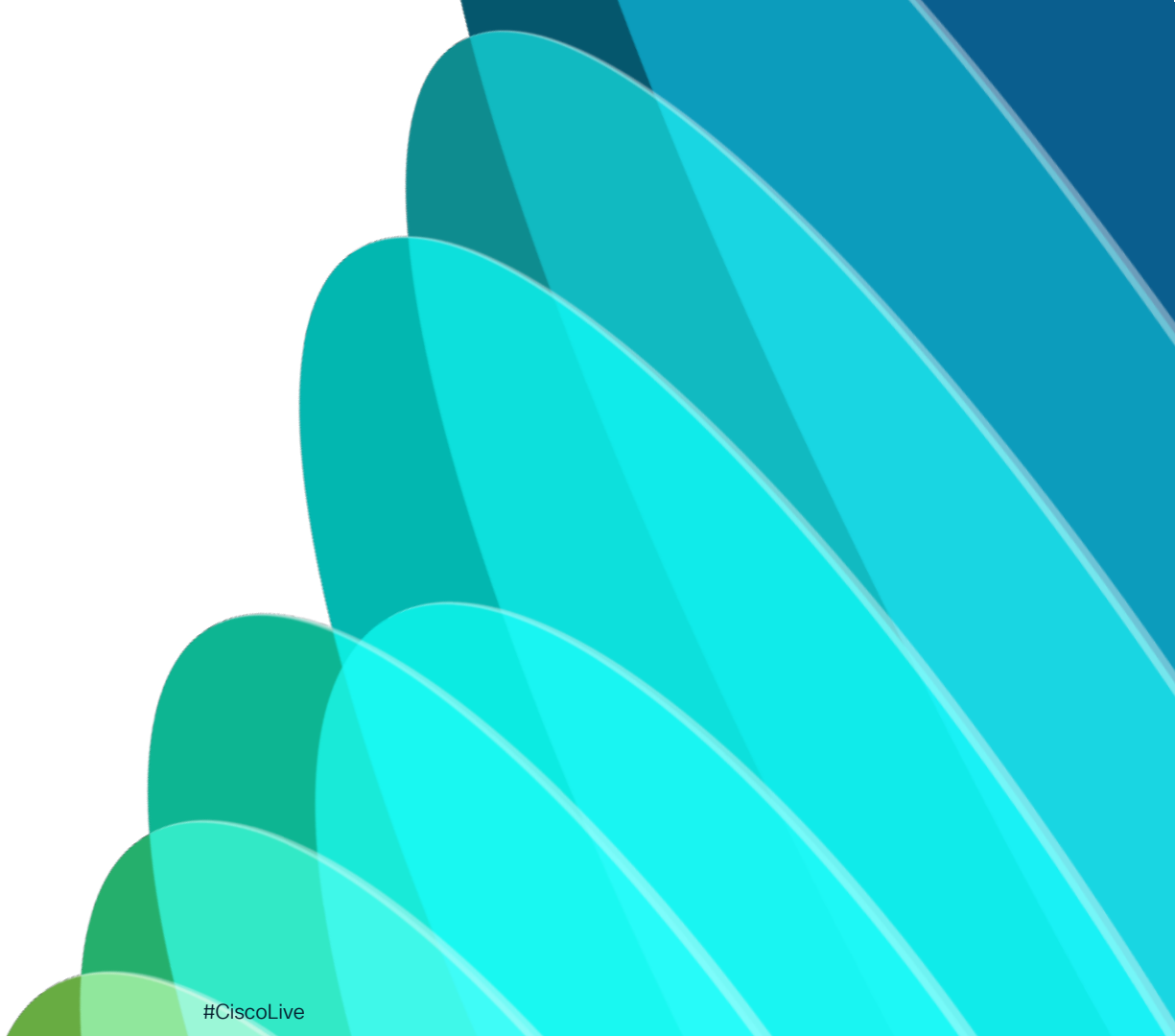
Complete your surveys in the **Cisco Live mobile app.**

Q & A



The bridge to possible

Thank you



cisco Live!

#CiscoLive